AI LAW, PLC
Ahmed Ibrahim, State Bar No. 238739
4343 Von Karman Ave, Suite 250
Newport Beach, CA 92660
Ph.: 949-260-1240
Fax: 949-260-1280
aibrahim@ailawfirm.com

Attorneys for Plaintiff, Individually and On Behalf of All Others Similarly Situated

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ARIFUR RAHMAN, an individual, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

MARRIOTT INTERNATIONAL, INC., a Delaware Corporation, DOES 1-100, inclusive,

Defendants.

CASE NO.: 8:20-cv-00654

CLASS ACTION COMPLAINT FOR:

(1) NEGLIGENCE

(2) VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT (Cal. Civ. Code § 1798.150)

(3) BREACH OF CONTRACT

(4) BREACH OF IMPLIED CONTRACT

(5) UNJUST ENRICHMENT

(6) VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE § 17200, *et seq.*)

DEMAND FOR JURY TRIAL

Plaintiff Arifur Rahman ("Plaintiff"), on behalf of himself and all others similarly situated, hereby alleges as follows:

I. BACKGROUND

1. This action arises out of a massive cybersecurity breach affecting 5.2 million consumers who entrusted their highly sensitive personal and confidential information to defendant Marriott International, Inc. ("Marriott"). Marriott announced the data breach on March 31, 2020 and sent e-mails to customers affected by the security debacle, informing them that information such as names, addresses, phone numbers, and e-mail addresses—all information that is solid gold for identity thieves—were accessed by unauthorized persons. This catastrophic and inexcusable mishap was unmistakably the result of Marriott's complete failure to exercise reasonable care and implement adequate security systems, institute the most basic cybersecurity policies and procedures, and adequately train employees and franchisees on such policies and procedures. In this action, Plaintiff, on behalf of a class of similarly situated California residents, seeks to hold Marriott accountable for its utter disregard for the privacy and sanctity of its customer's data—data that Marriott does not hesitate to take from customers for marketing analytics to upsell and increase revenues and to even share with third-parties, while making $20 Billion in revenue. Fortunately for consumers, the legislature passed the California Consumer Privacy Act (Cal. Civ. Code § 1791.100, *et seq.*) so that companies may finally learn their lesson when it comes to securing consumer data and being honest with them about what they are doing with that data. Indeed, it is no coincidence that the Act confers on private citizens the ability to bring civil actions for the failures of companies like Marriott to protect sensitive consumer data from a breach like the one at issue here. Plaintiff and the class members intend to vindicate those rights in this case.

II. PARTIES

2. Plaintiff Arifur Rahman ("Plaintiff") is an individual who is a citizen of the

State of California and resident of the County of Orange.

3. Defendant Marriott International, Inc. ("Marriott" or "Defendant") is a Delaware corporation with its principal place of business in Bethesda, Maryland.

4. The true names and capacities of defendants DOES 1 through 100, inclusive, whether individual, plural, corporate, partnership, associate or otherwise, are not known to Plaintiff, who therefore sues said defendants by such fictitious names. Plaintiff is informed and believes and thereon alleges that each of the defendants designated herein as DOE is in some manner responsible for the acts and occurrences set forth herein. Plaintiff will seek leave of court to amend this Complaint to show the true names and capacities of defendants DOES 1 through 100, inclusive, as well as the manner in which each DOE defendant is responsible, when the same have been ascertained.

5. Plaintiff is informed and believes, and upon such basis alleges, that at all times herein mentioned, each of the defendants herein was an agent, servant, employee, co-conspirator, partner, joint venturer, wholly owned and controlled subsidiary and/or alter ego of each of the remaining defendants, and was at all times acting within the course and scope of said agency, service, employment, conspiracy, partnership and/or joint venture.

6. Defendants, and each of them, aided and abetted, encouraged and rendered substantial assistance in accomplishing the wrongful conduct and their wrongful goals and other wrongdoing complained of herein. In taking action, as particularized herein, to aid and abet and substantially assist the commission of these wrongful acts and other wrongdoings complained of, each of the defendants acted with an awareness of its primary wrongdoing and realized that its conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals, and wrongdoing.

III. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 and 28 U.S.C. section 1332 because the total matter in controversy exceeds $5 Million and there are over 100 members of the proposed class.

Further, at least one member of the proposed class is a citizen of a State different from at least one defendant.

8. Venue is proper pursuant to 28 U.S.C. section 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this judicial district. Venue is also proper pursuant to 28 U.S.C. section 1391(b)(1) and (c)(2) because Defendant Marriott is subject to the Court's personal jurisdiction in this judicial district.

IV. GENERAL ALLEGATIONS

A. Company Background.

9. Marriott International is a multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, including 30 brands with more than 7,000 properties across 130 countries and territories globally. Marriott has a broad presence throughout California, where there are numerous Marriott properties. Founded in 1927, the company is headquartered in Bethesda, Maryland, and maintains hotel brands including Marriott, Courtyard, and Ritz-Carlton. Marriott reported revenues of $20.97 billion in the 2019 fiscal year.

10. Guests make reservations to stay at Marriott hotels in multiple ways, including through Marriott's website, http://www.marriott.com. When making a reservation, Marriott requires guests to provide certain personal information including name, address, email address, phone number, and payment card information. In some instances, Marriott also collects passport information, room preferences, travel destinations, and other personal information. Similarly, when creating an account to become a member of Marriott's customer loyalty program ("Marriott Bonvoy"), guests provide much of the same information specified above, as well as additional personal information such as date of birth and loyalty numbers of Marriott partners (e.g., airlines). Collectively, this information shall be referred to hereafter as "Personal Information." This Personal Information resides on databases maintained by Marriott and from which Marriott derives numerous benefits, including the ability to analyze the data to enhance their abilities to upsell and market hotels

and resorts to their guests, as well as in some cases, obtain direct monetary benefits for sharing data with third parties.

11. Personal Information provided by customers is governed by Marriott's Global Privacy Statement, which provides detailed information about what types of Personal Information will be shared, with what entities, and how it is collected. In its Global Privacy Statement dated June 3, 2019, Marriott assures customers that "[t]he Marriott Group, which includes Marriott International, Inc. . . . values you as our guest and recognizes that privacy is important to you." It states that the Marriott Group collects data:

(a) through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group.

(b) through the software applications made available by us for use on or through computers and mobile devices.

(c) through our social media pages that we control from which you are accessing this Privacy Statement

(d) through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us when you visit or stay as a guest at one of our properties, or at homes and villas offered on the Homes and Villas by Marriott International platform, or through other offline interactions.

12. In a section of the Global Privacy Statement entitled "Collection of Personal Data," Marriott Group communicates to customers that "[a]t touchpoints throughout your guest journey, we collect Personal Data in accordance with law[.]" Marriott Group defines "Personal Data" as "data that identify you as an individual or relate to an identifiable individual." This includes, according to Marriott Group:

- Name
- Gender
- Postal address
- Telephone number

- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

13. "In more limited circumstances," Marriott Group communicates to customers that it may also collect:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences, enquiries and comments and any other personalized data, such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit

14. This data is collected in a variety of ways, according to Marriott Group, including through online services, property visits and offline interactions, customer care centers, owners and franchisees, homes and villas property management companies, authorized licensees, strategic business partners, joint marketing partners, Internet-connected devices, and physical and mobile location-based services.

15. In a section of the Global Privacy Statement entitled "Security," Marriott Group claims that "[w]e seek to use reasonable organizational, technical and administrative measures to protect Personal Data."

16. In addition to this Global Privacy Statement, Marriott published on January 1, 2020 a statement specific to California residents on its website, entitled the "California Consumer Privacy Statement." In it, Marriott Group purports to provide what it refers to as "additional details" concerning the "the categories of Personal Information about California residents that we have collected or disclosed within the preceding 12 months[.]" It states that it collects the "following categories of Personal Information" from California residents:

(a) Identifiers, such as name, nationality, passport, visa or other government-issued identification data, and online identifiers;

(b) Personal information, as defined in the California safeguards law, such as name, contact information, and financial information;

(c) Characteristics of protected classifications under California or federal law, such as gender, age, medical conditions, primary language, national origin, citizenship, and marital status;

(d) Commercial information, such as transaction information, purchase history, financial details, payment methods, and membership or loyalty program data.

17. Marriott Group further states that in more limited circumstances, it may also collect the following categories of "Personal Information":

(a) Internet or network activity information, such as browsing history and interactions with our and other websites and computer systems;

(b) Geolocation data, such as device location and IP location;

(c) Audio, electronic, visual and similar information, such as images and

audio, video or call recordings created in connection with our business activities;

(d) Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

18. Marriott recognizes the value of this personal information of customers as evidenced by the fact that Marriott employs a customer analytics company for the systematic examination of its customer information to identify, attract, and retain the most profitable customers and to predict future behaviors. According to Marriott, "there is no lack of available data: household profile, including number of kids; type of jobs held by family members; their salaries; where and how they spend their money and even the type of jeans they buy." D. Eisen, *Marriott Bets on Predictive Analytics for Brand Growth*, QUESTEX LLC (Jan. 31, 2018), https://www.hotelmanagement.net/tech/marriott-builds-its-brands-by-knowing-more-about-you

19. Plaintiff and the class members provided their Personal Information to Marriott with the expectation and understanding that Marriott would adequately protect and store their data. If they had known that Marriott's data security was insufficient to protect their Personal Information, they would not have entrusted their Personal Information to Marriott and would not have been willing to pay for, or pay as much for, hotel reservations at Marriott properties and other amenities. Despite collecting the Personal Information of millions of consumers worldwide and, more specifically, of California consumers, Marriott failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly-sensitive databases. Marriott had the resources to prevent a breach and made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the hospitality and similar industries.

B. The Data Breach.

20. On March 31, 2020, Marriott announced a data breach affecting **5.2 million** customers in a statement posted on its website entitled "Marriott International: Incident

Notification." In the posting, Marriott stated that at the end of February 2020, Marriott "identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property." According to Marriott, "[w]e believe this activity started in mid-January 2020." Marriott claimed that upon discovery, it confirmed that the login credentials were disabled and it began an investigation—an investigation that Marriott admits is "ongoing" and thus has not been completed.

21. Marriott admits that "[a]t this point, we believe that the following information may have been involved," claiming that not all of the information was present for every guest involved:

- Contact details (e.g., name, mailing address, email address, and phone number)
- Loyalty Account Information (e.g., account number and points balance)
- Additional Personal Details (e.g., company, gender, and birthday day and month)
- Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers)
- Preferences (e.g., stay/room preferences and language preference)

22. In answering the question "How many guests were involved in this incident?" Marriott states "Although Marriott's investigation is ongoing, the company currently believes that information may have been involved for up to approximately 5.2 million guests."

23. Although Marriott contends in the statement that it "currently has no reason to believe" that other information was breached, it does not and cannot say so definitively and, as noted above, advised customers that its investigation is "ongoing."

24. Marriott also directed customers to a "self-service online portal" that it set up to enable guests "to determine whether their information was involved in the incident and, if so, what categories of information were involved." The portal was made accessible to customers via a hyperlink that redirected guests to a purportedly secure site where

customers could enter their name, e-mail address, country or region, and their customer loyalty program number (optional) to obtain more information about whether they were a victim of the data breach.

C. Plaintiff Is A Confirmed Victim of the Data Breach.

25. Plaintiff is a Marriott Bonvoy member and has spent money on many occasions to stay at Marriott properties. In connection with his Marriott Bonvoy account, along with making guest reservations to stay at Marriott properties and making purchases from said properties, Plaintiff has entrusted a litany of Personal Information to Marriott, and Marriott has collected and stored such information from Plaintiff, including, without limitation, his name, address, e-mail address, phone number, date of birth, and payment information.

26. On March 31, 2020, Plaintiff and other affected customers, including the members of the class, received a signed e-mail from Stephanie C. Linnartz, Marriott's Group President, Consumer Operations, Technology and Emerging Businesses. In the e-mail, Ms. Linnartz notified Plaintiff and other customers of the data security breach and advised them that their personal information may have been compromised. She stated: "We are writing to let you know that some of your information may have been accessed without authorization. We are sorry that this occurred, and this message explains what happened, how we can assist you, and steps you can take."

27. The remainder of the e-mail was similar to the announcement described above that was posted on Marriott's website the same day with one important and notable exception. Unlike the website posting, the e-mail sent to customers did *not* advise them that they could access a "self-service portal" where they would be able to determine whether their information was accessed in the breach. Rather, in what was obviously a cheap ploy to make it more unlikely that customers would find out whether their data had been stolen, Marriott put its customers through their paces. They made them first read the initial e-mail, then find the link to the announcement at http://mysupport.marriott.com, then re-read the announcement (which on its face appeared identical to the e-mail), find the

sentence relating to the portal (if they noticed it at all), click on the portal link, enter the information requested, receive a notification e-mail from the portal, and then return back to the portal to view the message.

28. After visiting the portal and entering the information requested, Plaintiff received a notification to his e-mail address prompting him to return to the portal to open a message he received. Shortly thereafter, Plaintiff received in the portal a message from the "Privacy Team" at the "Marriott Privacy Center" confirming that his personal data had, in fact, been involved in the data security breach. The message to Plaintiff states, in relevant part (with emphasis added), the following:

> We are in receipt of your inquiry regarding whether your personal data was involved in the property system incident that was announced in March 2020 (the Incident).
>
> Based on the email address and/or Marriott Bonvoy number that you provided to us, **we believe that your information was involved.** Following our analysis, **we currently believe that the following categories of information about you were involved in the Incident**
>
> **Contact details** (e.g., **name, mailing address, email address, and phone number**), Additional personal details (e.g., company, **gender, and birthday day and month**), Loyalty account information (e.g., **account number** and points balance, but not passwords), Partnerships and affiliations (e.g., **linked airline loyalty programs and numbers**), Preferences (e.g., stay/room preferences and language preference)

29. The fact that Plaintiff's and class members' Personal Information was accessed without authorization establishes that Marriott did not take adequate data security measures to store and protect its guests' Personal Information. Marriott failed to take adequate security measures to protect Plaintiff's and the class members' Personal Information.

D. <u>The Effects of the Data Breach on Victims of Marriott's Data Breach.</u>

30. Marriott's failure to keep Plaintiff's and class members' Personal Information secure has severe ramifications. Given the sensitive nature of the Personal Information

stolen in the Marriott data security breach at issue, including names, addresses, phone numbers, e-mail addresses, dates of birth, and account numbers—hackers have the ability to commit identity theft and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

31. The Personal Information exposed is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground Internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come.

32. Personal Information of the type breached in this case has significant monetary value in part because criminals continue their efforts to obtain this data. *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE, Sept. 28, 2014, available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html. In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018. *See* Identity Theft Center, *2019 End-of-Year Data Breach Report*, available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

33. It is not surprising that hotels have been frequent targets for hackers. As noted by one cybersecurity expert, "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries, like banking." Democrat-Gazette Staff Wire Reports, *Breach Puts Hotel Guests' Data at Risk*, ARKANSAS DEMOCRAT GAZETTE (Dec. 1, 2018),

https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/

34. The Personal Information of the type exposed in the data breach here remains of high value to identity criminals, as evidenced by the prices criminals will pay through black-market sources on the dark web. Numerous sources cite dark web pricing for stolen identity credentials, quantifying the loss to victims based on the value of the data itself. *Here's How Much Thieves Make By Selling Your Personal Data Online*, BUSINESS INSIDER (May 27, 2015), available at http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

35. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017 alone, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs. Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

36. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year. Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

37. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of personal information, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014. U.S. Department of Justice, Victims of Identity Theft, 2014 (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf.

38. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages. Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf.

39. Evidence shows identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

40. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.

41. There may also be a significant time lag between when personal information

is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf

42. Plaintiffs and the Class (as defined below) would not have provided their account information and other Personal Information to Marriott if they had known Marriott did not have in place adequate policies and procedures to protect their Personal Information.

43. As the result of Marriott's data breach, Plaintiff and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- Potentially having to purchase services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Marriott's substandard data security practices;
- losing the inherent value of their Personal Information;
- identity theft and fraud resulting from theft of their Personal Information;
- costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Marriott data breach, including discovering fraudulent charges, cancelling and

reissuing cards, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the data breach; and

- the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being in the possession of one or more unauthorized third parties.

44. Additionally, Plaintiff and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach. FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html.

45. Accordingly, had consumers known the truth about Marriott's data security practices—that Marriott would not adequately protect and store their data—they would not have entrusted their Personal Information to Marriott, created a Marriott Bonvoy account, and would not have been willing to pay for, or pay as much for, hotel stays at Marriott. As such, Plaintiff and class members did not receive the benefit of their bargain with Marriott because they paid for a value of services, either through Personal Information or a combination of their Personal Information and money, they expected but did not receive.

V. CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action on behalf of himself and all persons similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure and seeks certification of the following class:

> All persons in the State of California whose Personal Information was stolen, disclosed, or accessed without authorization in the data breach incident Marriott announced on

March 31, 2020.

47. The above-described class of persons shall hereafter be referred to as the "Class." Excluded from the Class are Marriott's officers, directors, legal representatives, successors, subsidiaries, and assigns, and any judge who presides over this action.

48. Plaintiff reserves the right to expand, limit, modify, or amend the class definitions stated above, including the addition of one or more subclasses, in connection with his motion for class certification, or at any other time, based upon, among other things, changing circumstances, or new facts obtained during discovery.

49. **Numerosity.** The Class is so numerous that joinder of all members in one action is impracticable. The exact number and identities of the members of the Class is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, but on information and belief, Plaintiff alleges that there are in excess of 1 Million members of the Class.

50. **Typicality.** Plaintiff's claims are typical of those of other members of the Class, all of whom have suffered similar harm due to Defendants' course of conduct as described herein.

51. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class. Plaintiff has retained attorneys who are experienced in the handling of complex litigation and class actions, and Plaintiff and his counsel intend to prosecute this action vigorously.

52. **Existence and Predominance of Common Questions of Law or Fact.** Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary among members of the Class, and which may be determined without reference to the individual circumstances of any member of the Class, include, but are not limited to, the following:

(a) Whether Marriott owed a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to protect their Personal Information;

(b) Whether Marriott violated its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information of Plaintiff and members of the Class.

(c) Whether the Personal Information compromised in the data breach was information that is protected by California law;

(d) Whether Marriott knew or should have known that its computer and data storage systems were vulnerable to attack;

(e) Whether Marriott failed to take available steps to prevent and stop the data breach from occurring;

(f) Whether Marriott's failure to secure Plaintiff's and the Class's Personal Information in the manner alleged violated federal, state and local laws, or industry standards;

(g) Whether Marriott's conduct, including its failure to act, resulted in or was the proximate cause of the data breach, resulting in the unauthorized access to and/or theft of Plaintiff's' and the Class's Personal Information;

(h) Whether Marriott has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

(i) Whether Marriott's conduct amounted to violations of California consumer protection statutes, and/or California data breach statutes;

(j) Whether, as a result of Marriott's conduct, Plaintiff and members of the Class face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

(k) Whether, as a result of Marriott's conduct, Plaintiff and members of the Class are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

53. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy, because individual litigation of the claims of all members of the Class is impracticable. Requiring each individual class member to file an individual lawsuit would unreasonably consume the amounts that may be recovered. Even if every member of the Class could afford individual litigation, the adjudication of at least tens of thousands of identical claims would be unduly burdensome to the courts.

Individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the conduct of this action as a class action, with respect to some or all of the issues presented herein, presents no management difficulties, conserves the resources of the parties and of the court system, and protects the rights of the members of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. The prosecution of separate actions by individual members of the Class may create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of the other members of the Class not parties to such adjudications or that would substantially impair or impede the ability of such non-party Class members to protect their interests.

54. **Ascertainability.** Defendant keeps extensive computerized records of their customers through, among other things, databases storing customer reservations and stays, customer histories, customer profiles, the Marriott Bonvoy customer loyalty program, and general marketing programs. Defendant has one or more databases through which a significant majority of members of the Class may be identified and ascertained, and they maintain contact information, including email addresses and home addresses (such as billing, mailing, and shipping addresses), through which notice of this action is capable of being disseminated in accordance with due process requirements.

COUNT ONE

NEGLIGENCE

(By Plaintiff Against Defendants on Behalf of the Class)

55. Plaintiff restates and re-alleges paragraphs 1 through 54 as if fully set forth herein.

56. Marriott required Plaintiff and the Class to submit sensitive Personal Information in order to make and pay for reservations at Marriott properties and/or obtain access to the Marriott loyalty program (Marriott Bonvoy). Marriott stored this sensitive

and valuable Personal Information on its computer and data storage systems.

57. By collecting, storing, using, and profiting from this data, Marriott had a duty of care to Plaintiff and the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this Personal Information in Marriott's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Marriott's security systems and data storage architecture to ensure that Plaintiff and the Class's Personal Information was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Marriott's security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Marriott's security vulnerabilities and potential compromise of the compiled data of Plaintiff and the Class; (d) maintaining and implementing data security measures consistent with industry standards; and (e) instituting data security policies and procedures, and adequately training employees and franchisees on such policies and procedures.

58. Marriott had common law duties to prevent foreseeable harm to Plaintiff and the Class. These duties existed because Plaintiff and members of the Class were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and the Class would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Marriott knew that it was more likely than not Plaintiff and other class members would be harmed by such theft.

59. Marriott had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the Personal Information that was collected and stored on Marriott's computer systems.

60. Marriott's duties to use reasonable security measures also arose as a result of the special relationship that existed between Marriott, on the one hand, and Plaintiff and members of the Class, on the other hand. The special relationship arose because Plaintiff

and members of the Class entrusted Defendant with their Personal Information in order to make and pay for reservations at Marriott properties and/or create user accounts necessary to access the Marriott Bonvoy program. Marriott alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the data breach.

61. Marriott knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Personal Information.

62. Marriott breached the duties it owed to Plaintiff and class members described above and thus were negligent. Marriott breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and the Class; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) institute data security policies and procedures, and adequately train employees and franchisees on such policies and procedures.

63. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiff and the Class members, their Personal Information would not have been compromised.

64. As a direct and proximate result of Marriott's negligence, Plaintiff and the Class have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the data breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value

of the Personal Information; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT TWO

VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT (CAL. CIV CODE § 1798.100, *et seq.*)

(By Plaintiff Against Defendants on Behalf of the Class)

65. Plaintiff restates and re-alleges paragraphs 1 through 64 as if fully set forth herein.

66. The California Consumer Privacy Act ("CCPA"), portions of which were operative beginning January 1, 2020, was enacted by the California Legislature "to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80)." Cal. Civ. Code § 1798.100. The CCPA applies to "the collection and sale of all personal information collected by a business from consumers." *Id.*

67. "Businesses," defined to include a "corporation" that "collects consumers' personal information" that "does business in the State of California" and has annual gross revenues in excess of $25 million, are required to comply with the CCPA. Cal. Civ. Code § 1798.140(c). Marriott is a "business" under the CCPA.

68. The CCPA protect "consumers." "Consumer" is defined as "a natural person who is a California resident[.]" Cal. Civ. Code § 1798.140(g). Plaintiff and members of the Class are "consumers" within the meaning of the CCPA.

69. The protections of the CCPA extend to "personal information" of consumers. "Personal information" is defined by the CCPA to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1). "Personal information includes, but is not limited to, the following if it

identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a *real name*, alias, *postal address*, unique personal identifier, online identifier, internet protocol address, *email address*, *account name*, social security number, driver's license number, passport number, or other similar identifiers." Cal. Civ. Code § 1798.140(o)(1)(A) (emphasis added). It may also include a "telephone number," Cal. Civ. Code § 1798.140(o)(1)(B), Cal. Civ. Code § 1798.80(e), as well as "[c]ommercial information, including . . . products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies" and "[p]rofessional or employment-related information." Cal. Civ. Code § 1798.140(o)(1)(D) & (I). The Personal Information of Plaintiff and members of the Class that was compromised in Marriott's data breach included "personal information" within the meaning of the CCPA.

70. The CCPA provides consumers with the right to institute a civil action where the consumers' "nonencrypted and nonredacted personal information" was the subject of "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information . . ." Cal. Civ. Code § 1798.150(a)(1).

71. Marriott, as a "business" covered by the CCPA, owed a duty to Plaintiff and members of the Class to implement and maintain reasonable security procedures and practices" to protect the Personal Information of Plaintiff and members of the Class.

72. Marriott breached this duty. On March 31, 2020, Marriott announced a data breach affecting 5.2 million customers, a large portion of whom are members of the Class. Marriott admitted that at the end of February 2020, it "identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property." According to Marriott, "[w]e believe this activity started in mid-January 2020." Marriott also admitted that contact details (e.g., name, mailing address, email address, and phone number), Loyalty Account Information (e.g., account number

and points balance), additional personal details (e.g., company, gender, and birthday day and month), partnerships and affiliations (e.g., linked airline loyalty programs and numbers), and preferences (e.g., stay/room preferences and language preference) may all have been accessed in the breach.

73. With regard to Plaintiff, Marriott apologized to him and admitted that his personal information was accessed without his authorization, including, his contact details (e.g., name, mailing address, email address, and phone number), additional personal details (e.g., company, gender, and birthday day and month), loyalty account information (e.g., account number and points balance), partnerships and affiliations (e.g., linked airline loyalty programs and numbers), and preferences (e.g., stay/room preferences and language preference)."

74. The fact that Plaintiff's and the Class's Personal Information was accessed without authorization establishes that Marriott did not take adequate data security measures to store and protect its guests' Personal Information. Marriott failed to take adequate security measures to protect Plaintiff's and the class members' Personal Information.

75. As a direct and proximate result of Marriott's acts and omissions, Plaintiff and the members of the Class were subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of the duty.

76. On behalf of the Class, Plaintiff seeks injunctive relief in the form of an order (a) enjoining Marriott from continuing to violate the CCPA, (b) requiring Marriott to employ adequate security practices consistent with law and industry standards to protect class members' personal information, (c) requiring Marriott to complete its investigation, and (d) issuing an amended statement to the public and affected guests that is not evasive and contains no equivocations (e.g., phrases such as "may have," the investigation is "ongoing," "no reason to believe," etc.) and to instead confirm and confess, with certainty, what categories of data were stolen and accessed without class members' authorization, how the data breach occurred, and what specifically occurred to cause the breach.

77. Plaintiff presently seeks only injunctive relief and any other relief the court

deems proper pursuant to this section, such as attorneys' fees. Prior to initiating this action, Plaintiff served written notice identifying Marriott's violations of section 1798.150(a) and demanding that the data breach be cured. If within 30 days, Marriott has not cured, Plaintiff will amend this Complaint to seek statutory damages pursuant to Civil Code section 1798.150(a)(1)(A).

COUNT THREE

BREACH OF CONTRACT

(By Plaintiff Against Defendants on Behalf of the Class)

78. Plaintiff restates and re-alleges paragraphs 1 through 77 as if fully set forth herein.

79. Marriott's Global Privacy Statement dated June 3, 2019 and its California Privacy Statement dated January 1, 2020 (together, the "Privacy Policy") is an agreement between Marriott and persons who provide their Personal Information to Marriott, including Plaintiff and the Class.

80. The Global Privacy Statement, as it was in effect at the time of the Marriott data breach, applies to persons from whom Marriott has collected Personal Information. When read together with the California Privacy Statement, the two documents apply to California residents from whom Marriott has collected Personal Information.

81. The Privacy Policy provides detailed information about what types of Personal Information will be shared, with what entities, and how it is collected. Marriott assures customers, including Plaintiff and the Class, that "[t]he Marriott Group, which includes Marriott International, Inc. . . . values you as our guest and recognizes that privacy is important to you." Marriott Group also assures customers, including Plaintiff and the Class, that "[w]e seek to use reasonable organizational, technical and administrative measures to protect Personal Data." Further, Marriott delineates in the Privacy Policy the universe of persons and entities who are authorized to receive Personal Information of customers, including Plaintiff and the Class, and what specific categories of Personal

Information they are authorized to receive. Any disclosures of Personal Information that deviate from the Privacy Policy are not authorized disclosures.

82. Plaintiff and members of the Class, on the one hand, and Marriott on the other hand, formed a contract when Plaintiff and members of the Class members provided Personal Information to Marriott subject to the Privacy Policy.

83. Plaintiff and the Class fully performed their obligations under the contract with Marriott.

84. Marriott breached its agreement with Plaintiff and the Class by failing to protect their Personal Information and permitting disclosures of Personal Information that deviated from, and were inconsistent with, the Privacy Policy. Specifically, Marriott (1) failed to use reasonable measures to protect that Personal Information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

85. As a direct and proximate result of these breaches of contract, Plaintiff and the Class sustained actual losses and damages as described in detail above, including but not limited to, that they did not get the benefit of the bargain pursuant to which they provided their Personal Information to Marriott.

COUNT FOUR

BREACH OF IMPLIED CONTRACT

(By Plaintiff Against Defendants on Behalf of the Class)

86. Plaintiff restates and re-alleges paragraphs 1 through 85 as if fully set forth herein.

87. Plaintiff and the Class also entered into an implied contract with Marriott when they obtained services from Marriott, or otherwise provided Personal Information to Marriott.

88. As part of these transactions, Marriott agreed to safeguard and protect the Personal Information of Plaintiff and the Class.

89. Plaintiff and members of the Class entered into implied contracts with the

reasonable expectation that Marriott's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and the Class believed that Marriott would use part of the monies paid to Marriott, or monies which it derived from sharing the Personal Information with third parties, under the implied contracts to fund adequate and reasonable data security practices.

90. Plaintiff and the Class would not have provided and entrusted their Personal Information to Marriott or would have paid less for Marriott's services in the absence of the implied contract or implied terms between them and Marriott. The safeguarding of the Personal Information of Plaintiffs and class members was critical to realize the intent of the parties.

91. Plaintiff and the Class fully performed their obligations under the implied contracts with Marriott.

92. Marriott breached its implied contracts with Plaintiff and the Class to protect their Personal Information when it (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

93. As a direct and proximate result of these breaches of implied contract, Plaintiff and the Class sustained actual losses and damages as described in detail above, including but not limited to, that they did not get the benefit of the bargain pursuant to which they provided their Personal Information to Marriott.

COUNT FIVE

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE § 17200, *et seq.*)

(By Plaintiff Against Defendants on Behalf of the Class)

94. Plaintiff restates and re-alleges paragraphs 1 through 93 as if fully set forth herein.

95. California Business and Professions Code section 17200 *et seq.*, also known

as the California Unfair Competition Law ("UCL"), prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice."

96. A cause of action may be brought under the "unlawful" prong of the UCL if a practice violates another law. Such an action borrows violations of other laws and treats these violations, when committed pursuant to business activity, as unlawful practices independently actionable under the UCL.

97. Here, Marriott's "unlawful" acts and practices include violating California Civil Code section 1798.150 as described above, and failing to implement and maintain reasonable security measures contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

98. A business act or practice is "unfair" under the UCL if it offends an established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers, and that unfairness is determined by weighing the reasons, justifications and motives of the practice against the gravity of the harm to the alleged victims.

99. Here, Marriott's "unfair" acts and practices include:

(a) failing to abide by the provisions of California Civil Code section 1798.150

(b) failing to implement and maintain reasonable security measures contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

(c) failing to implement and maintain reasonable security measures to protect Plaintiff's and the Class's Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the data breach.

Marriott failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the Class, whose Personal Information has been compromised; and

(d) failing to implement and maintain reasonable security measures, which also led to substantial consumer injuries, as described above, and which are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Marriott's inadequate security, consumers could not have reasonably avoided the harms that Marriott caused.

100. A business act or practice is "fraudulent" within the meaning of the UCL if members of the public are likely to be deceived.

101. Here, Marriott's "fraudulent" acts and practices include:

(a) misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Class's Personal Information, including by implementing and maintaining reasonable security measures;

(b) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Class's Personal Information; and

(c) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Class's Personal Information, including duties imposed by the CCPA and the FTC Act.

102. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information.

103. As a direct and proximate result of Marriott's unfair, unlawful, and fraudulent acts and practices, Plaintiff and the Class were injured and lost money or property, including, but not limited to: the money received by the Marriott for its services; the loss of the benefit of their bargain with and overcharges by Marriott as they would not have

paid Marriott for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; any costs they will have to incur for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

104. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Marriott's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure section 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT SIX

UNJUST ENRICHMENT

(By Plaintiff Against Defendants on Behalf of the Class, or in the Alternative, the California Class)

105. Plaintiff restates and re-alleges paragraphs 1 through 104 as if fully set forth herein.

106. Plaintiff and the Class have an interest, both equitable and legal, in the Personal Information about them that was furnished to, collected by, and maintained by Marriott and that was ultimately stolen in the data breach.

107. Marriott was benefited by the conferral upon it of the Personal Information pertaining to Plaintiff and the Class and by its ability to retain, use, and profit from that information. Marriott understood that it was in fact so benefited.

108. Marriott also understood and appreciated that the Personal Information pertaining to Plaintiff and the Class was private and confidential and its value depended upon Marriott maintaining the privacy and confidentiality of that Personal Information.

109. But for Marriott's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted

with Marriott.

110. Marriott continues to benefit and profit from its retention and use of the Personal Information while its value to Plaintiff and the Class has been diminished.

111. Marriott also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff' and the Class's Personal Information.

112. It is inequitable for Marriott to retain these benefits.

113. As a result of Marriott's wrongful conduct as alleged in this Complaint (including, among other conduct, its knowing failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Marriott has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

114. Marriott's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff' and class members' Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

115. Under the common law doctrine of unjust enrichment, it is inequitable for Marriott to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Marriott's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

116. The benefits conferred upon, received, and enjoyed by Marriott were not conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to retain these benefits.

117. Plaintiff and the Class have no adequate remedy at law.

118. Marriott is therefore liable to Plaintiff and the Class for restitution or disgorgement in the amount of the benefit conferred on Marriott as a result of its wrongful

conduct, including specifically: the value to Marriott of the Personal Information that was stolen in the data breach; the profits Marriott is receiving from the use of that information; and the amounts that Marriott should have spent to provide reasonable and adequate data security to protect Plaintiffs' and class members' Personal Information.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the Class, prays for judgment against Defendants, and each of them, as follows:

1. For an order certifying that the action be maintained as a class action under Rule 23(b)(2), Rule 23(b)(3), and/or 23(c)(4) of the Federal Rules of Civil Procedure, that Plaintiff be designated the class representative, and that undersigned counsel be designated as class counsel.

2. For injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and members of the Class, including but not limited to an order:

(a) Prohibiting Marriott from engaging in the wrongful and unlawful acts described herein;

(b) Requiring Marriott to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

(c) Requiring Marriott to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and class members' Personal Information;

(d) Requiring Marriott to engage independent third-party security auditors and internal personnel to run automated security monitoring;

(e) Requiring Marriott to audit, test, and train its security personnel regarding any new or modified procedures;

(f) Requiring Marriott to segment data by, among other things, creating firewalls and access controls so that if one area of Marriott's network is compromised,

hackers cannot gain access to other portions of Marriott's systems;

(g) Requiring Marriott to conduct regular database scanning and security checks;

(h) Requiring Marriott to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiff and the Class;

(i) Requiring Marriott to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(j) Requiring Marriott to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor the Marriott's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

(k) Requiring Marriott to meaningfully educate all class members about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps affected individuals must take to protect themselves; and

(l) Requiring Marriott to implement logging and monitoring programs sufficient to track traffic to and from Marriott's servers.

3. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined at trial;

4. For an award of restitution or disgorgement, in an amount to be determined at trial;

5. For an award of attorneys' fees, costs, and litigation expenses pursuant to California Code of Civil Procedure section 1021.5 or as otherwise allowed by law;

6. For prejudgment interest on all amounts awarded; and

7. For such other and further relief as the Court may deem just and proper.

Dated: April 3, 2020 AI LAW, PLC

By: /s/ Ahmed Ibrahim
Ahmed Ibrahim
Attorneys for Plaintiff, Individually and
On Behalf of All Others Similarly Situated

JURY DEMAND

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: April 3, 2020 AI LAW, PLC

By: /s/ Ahmed Ibrahim
Ahmed Ibrahim
Attorneys for Plaintiff, Individually and
On Behalf of All Others Similarly Situated